

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :
Motoji OHMORI et al. :
Serial No. NEW : **Attn: APPLICATION BRANCH**
Filed July 17, 2003 : **Attorney Docket No. 2003_0831A**
SYSTEM FOR PREVENTING :
UNAUTHORIZED USE OF RECORDING :
MEDIA :

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

THE COMMISSIONER IS AUTHORIZED
TO CHARGE ANY DEFICIENCY IN THE
FEES FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975

Sir:

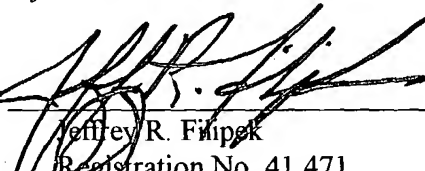
Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2002-208398, filed July 17, 2002, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Motoji OHMORI et al.

By


Jeffrey R. Filipek
Registration No. 41,471
Attorney for Applicants

JRF/fs
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
July 17, 2003

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :

Motoji OHMORI et al. :

Attn: APPLICATION BRANCH

Serial No. NEW :

Attorney Docket No. 2003_0831A

Filed July 17, 2003 :

SYSTEM FOR PREVENTING
UNAUTHORIZED USE OF RECORDING
MEDIA :

THE COMMISSIONER IS AUTHORIZED
TO CHARGE ANY DEFICIENCY IN THE
FEES FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975

**COVER LETTER FOR APPLICATION FILED
WITHOUT EXECUTED DECLARATION**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The above-identified application has been submitted without an executed oath or declaration pursuant to 37 CFR 1.41(c).

It is respectfully requested that this application be assigned a serial number and awarded a filing date pursuant to 37 CFR 1.53.

A duly executed oath or declaration pursuant to 37 CFR 1.63 will be submitted after notification by the U.S. Patent and Trademark Office pursuant to 37 CFR 1.52(d).

A non-executed copy of the Declaration and Power of Attorney, containing the inventorship information, is attached. It is respectfully requested that all communications be directed to the firm indicated on the attached Declaration and Power of Attorney, namely:

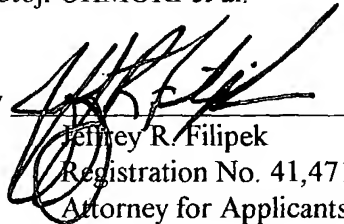
WENDEROTH, LIND & PONACK, L.L.P.
2033 K Street, N.W., Suite 800
Washington, D.C. 20006-1021

The required U.S. Patent and Trademark Office Filing Fee is submitted herewith.

Respectfully submitted,

Motoji OHMORI et al.

By

A handwritten signature in black ink, appearing to read "Jeffrey R. Filipek", is written over a horizontal line.

Jeffrey R. Filipek
Registration No. 41,471
Attorney for Applicants

JRF/fs
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
July 17, 2003

日 本 国 特 許 庁

JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 7月17日

出 願 番 号

Application Number:

特願2002-208398

[ST.10/C]:

[JP2002-208398]

出 願 人

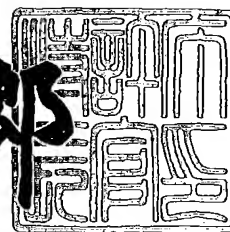
Applicant(s):

松下電器産業株式会社

2003年 1月21日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3000230

【書類名】 特許願

【整理番号】 2022540224

【提出日】 平成14年 7月17日

【あて先】 特許庁長官殿

【国際特許分類】 H04M 1/67

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 大森 基司

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 上田 健一

【発明者】

【住所又は居所】 広島県東広島市鏡山3丁目10番18号 株式会社松下電器情報システム広島研究所内

【氏名】 植田 栄治

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 記録媒体不正使用防止システム

【特許請求の範囲】

【請求項 1】 端末装置に着脱可能な記録媒体の不正使用防止システムであって、

前記記録媒体の使用の可否を決定する認証情報を複数記憶する第 1 記憶部と、
前記第 1 記憶部に記憶された認証情報に対応した処理手段を記憶する第 2 記憶部と、

前記記録媒体の利用者が有する利用者情報と前記認証情報とを用いて認証を行う認証部と、

前記認証部の認証の内容に対応して、前記処理手段を実行する処理部と、
を備えたことを特徴とする記録媒体不正使用防止システム。

【請求項 2】 前記記録媒体不正使用防止システムは、さらに前記端末装置の通信機能を使用するための通信情報を記憶する第 3 記憶部とを有し、

前記処理部は、前記通信情報と前記認証部の認証の内容とに対応した前記処理手段を実行することを特徴とする請求項 1 記載の記録媒体不正使用防止システム。

【請求項 3】 前記記録媒体不正使用防止システムは、さらに前記端末装置の通信機能を使用するための通信情報を複数記憶する第 4 記憶部と、

前記第 4 記憶部の通信情報から所望の通信情報を選択する選択部とを有し、
前記処理部は、前記選択部により選択された通信情報と前記認証部の認証の内容とに対応した前記処理手段を実行することを特徴とする請求項 1 記載の記録媒体不正使用防止システム。

【請求項 4】 前記不正使用防止システムは、さらに前記端末装置と前記記録媒体との着脱を判断する判断部を有し、

前記判断部により前記記録媒体が前記端末装置から抜き出されたことを認識した後、前記記録媒体を使用する場合には、前記認証部による認証を行うことを特徴とする請求項 1 乃至 3 記載の記録媒体不正使用防止システム。

【請求項 5】 前記不正使用防止システムは、さらに前記認証情報を設定する

認証情報設定部を有し、

前記認証情報設定部により設定された認証情報を第 1 記憶部に記憶することを特徴とする請求項 1 乃至 4 記載の記録媒体不正使用防止システム。

【請求項 6】 前記不正使用防止システムは、さらに前記処理手段を設定する処理手段設定部を有し、

前記処理手段設定部により設定された処理手段を第 2 記憶部に記憶することを特徴とする請求項 1 乃至 4 記載の記録媒体不正使用防止システム。

【請求項 7】 前記不正使用防止システムは、さらに前記通信情報を設定する通信情報設定部を有し、

前記通信情報設定部により設定された通信情報を第 3 又は第 4 記憶部に記憶することを特徴とする請求項 1 乃至 4 記載の記録媒体不正使用防止システム。

【請求項 8】 不正使用防止システムに使用する端末装置に着脱可能な記録媒体であって、

少なくとも前記記録媒体の使用の可否を決定する認証情報を複数記憶する第 1 記憶部と、

前記第 1 記憶部に記憶された認証情報に対応した処理手段を記憶する第 2 記憶部と、

を備えたことを特徴とする記録媒体。

【請求項 9】 前記記録媒体はさらに前記端末装置の通信機能を使用するための通信情報を記憶する第 3 記憶部を備えたことを特徴とする請求項 8 記載の記録媒体。

【請求項 10】 前記記録媒体はさらに前記端末装置の通信機能を使用するための通信情報を複数記憶する第 4 記憶部を備えたことを特徴とする請求項 8 記載の記録媒体。

【請求項 11】 前記記録媒体はさらに前記記録媒体の使用者の有する使用者情報と前記認証情報とを用いて認証を行う認証部と、

を備えた請求項 8 乃至 10 記載の記録媒体。

【請求項 12】 前記記録媒体はさらに前記端末装置と前記記録媒体との着脱を判断する判断部を有し、

前記判断部により前記記録媒体が前記端末装置から抜き出されたことを認識した後、前記記録媒体を使用する場合には、前記認証部による認証を行うことを特徴とする請求項 8 乃至 11 記載の記録媒体不正使用防止システム。

【請求項 13】 不正使用防止システムに使用する記録媒体が着脱可能な端末装置であって、

少なくとも前記記録媒体の使用の可否を決定する認証情報を複数記憶する第 1 記憶部と、

前記第 1 記憶部に記憶された認証情報に対応した処理手段を記憶する第 2 記憶部と、

前記端末装置の使用者の有する端末使用者情報と前記認証情報とを用いて認証を行う認証部と、

前記認証部の認証の内容に対応して前記処理手段を実行する処理部と、
を備えたことを特徴とする端末装置。

【請求項 14】 前記端末装置は、さらに前記端末装置の通信機能を使用するための通信情報を複数記憶する第 4 記憶部と、

前記第 4 記憶部の使用者識別情報から所望の使用者識別情報を選択する選択部とを有し、

前記処理部は、前記選択部により選択された通信情報と前記認証部の認証の内容に対応し前記処理手段を実行することを特徴とする請求項 13 記載の端末装置。

【請求項 15】 端末装置に着脱可能な記録媒体の不正使用防止方法であって

前記記録媒体の使用の可否を決定する認証情報を複数記憶する第 1 記憶工程と

前記第 1 記憶工程に記憶された認証情報に対応した処理手段を記憶する第 2 記憶工程と、

前記記録媒体の使用者が有する使用者情報と前記認証情報とを用いて認証を行う認証工程と、

前記認証工程の認証の内容に対応して、前記処理手段を実行する処理工程と、

を備えたことを特徴とする記録媒体不正使用防止方法。

【請求項 16】 端末装置に着脱可能な記録媒体の不正使用防止方法であって

前記記録媒体の使用の可否を決定する認証情報を複数記憶する第1記憶工程と

前記第1記憶工程に記憶された認証情報に対応した処理手段を記憶する第2記憶工程と、

前記端末装置の通信機能を使用するための通信情報を記憶する第3記憶工程と

前記記録媒体の利用者が有する利用者情報と前記認証情報とを用いて認証を行う認証工程と、

前記通信情報と前記認証工程の認証の内容とに対応した前記処理手段を実行する処理工程と、

を備えたことを特徴とする記録媒体不正使用防止方法。

【請求項 17】 端末装置に着脱可能な記録媒体の不正使用防止方法であって

前記記録媒体の使用の可否を決定する認証情報を複数記憶する第1記憶工程と

前記第1記憶工程に記憶された認証情報に対応した処理手段を記憶する第2記憶工程と、

前記端末装置の通信機能を使用するための通信情報を複数記憶する第4記憶工程と、

前記第4記憶工程の通信情報から所望の通信情報を選択する選択工程と、

前記記録媒体の利用者が有する利用者情報と前記認証情報とを用いて認証を行う認証工程と、

前記選択工程により選択された通信情報と前記認証工程の認証の内容とに対応した前記処理手段を実行する処理工程と、

を備えたことを特徴とする記録媒体不正使用防止方法。

【請求項 18】 請求項 15 から 17 の何れか一つに記載の方法を実行する記

録媒体不正使用防止プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、端末装置に対して着脱可能な記録媒体の不正使用防止に関するものである。

【0002】

【従来の技術】

携帯電話等の電子機器の分野において、近年、SIM (Subscriber Identity Module) カードと称される利用者識別カードを、電話機本体に装着して通信を行い得るようにするシステムが考えられている。そして、このSIMカードには、SIMカードの所有者の個人情報が記憶されている。このような構成とすることにより、電話機を所有しない者、あるいは自らの電話機が故障、電池切れ等で使用不能となった場合でも、他者の電話機あるいは公共の電話機を用いて、自己のSIMカードを装着することにより、使用者自身のIDコードを用いた通話を行うことができる。これにより、課金処理もSIMカードの所有者を対象として行うことができるようになる。さらに、自らの所有する電話機ではない場合でも、SIMカードに記憶されたメモリダイヤルのデータに基づいて電話をかけることも可能になる。

【0003】

【発明が解決しようとする課題】

しかしながら、このような便利なSIMカードであっても、紛失又は盗難等によりSIMカードが意図せず第三者に渡ってしまうことが考えられる。このような場合、そのSIMカードを取得した第三者の悪意により不正な使用がなされることも考えられる。

【0004】

また、一個人が複数のSIMカードを携帯する可能性も考えられ、紛失又は盗難による不正使用の可能性が高くなることも予想される。

【0005】

さらに、SIMカードのような携帯電話に着脱可能な記録媒体が、上述した通信機能に加えて、例えば、電子商取引等の機能を有することも考えられる。そのような場合には、紛失又は盗難による第三者の使用により、上述した記録媒体の所有者が、電子マネーが第三者により使用されることなどにより、さらに記録媒体の使用が深刻な事態に陥ることが予想される。

【0006】

本発明は、上記問題点を解決することによって、第三者の不正使用を防止し、記録媒体の所有者に安全且つ利便性の高い記録媒体を提供することを目的とする。

【0007】

【課題を解決するための手段】

上記の目的を達成するために、この発明の端末装置に着脱可能な記録媒体の不正使用防止システムは、前記記録媒体の使用の可否を決定する認証情報を複数記憶する第1記憶部と、前記第1記憶部に記憶された認証情報に対応した処理手段を記憶する第2記憶部と、前記記録媒体の使用が有する使用者情報と前記認証情報とを用いて認証を行う認証部と、前記認証部の認証の内容に対応して、前記処理手段を実行する処理部と、を含むことを特徴とする。これにより、処理手段の内容に対応して適切に第三者の使用を防止することが可能になる。

【0008】

また、前記不正使用防止システムは、さらに前記端末装置を使用するための通信情報を複数記憶する第4記憶部と、前記第4記憶部の通信情報から所望の通信情報を選択する選択部とを有し、前記処理部は、前記選択部により選択された通信情報と前記認証部の認証の内容とに対応した前記処理手段を実行する構成としてもよい。これにより、一個人が複数の電話番号を有する場合であっても、SIMカードのような記録媒体を複数携帯する必要がなく、記録媒体の利便性を向上させることができる。

【0009】

また、前記不正使用防止システムは、さらに前記端末装置と前記記録媒体の着脱を判断する判断部を有し、前記判断部により前記記録媒体が前記端末装置から

抜き出されたことを認識した後、前記記録媒体を使用する場合には、前記認証部による認証を行う構成としてもよい。これにより、第三者により記録媒体が前記端末装置から抜き出された場合であっても再度認証部による認証を行うため、第三者の不正使用を防止することが可能になる。

【0010】

【発明の実施の形態】

図1は、この発明の一実施の形態に係る端末装置から着脱可能な記録媒体の不正使用防止システム（以下、「記録媒体不正使用防止システム」とする。）の概略構成図である。

【0011】

この実施の形態の記録媒体不正使用防止システムは、端末装置100又は200と、端末装置100又は200から着脱可能な記録媒体300とを備えている。

【0012】

端末装置100又は200は、携帯型の電話機、PDA (Personal Digital Assistant)、パーソナルコンピュータ、カーナビゲーションシステム、FAX、デジタルカメラ（PDA、パーソナルコンピュータ、カーナビゲーションシステム、FAX、デジタルカメラは図示せず）等、記録媒体300が着脱可能な装置である。

【0013】

記録媒体300は、以下に述べる処理が可能であり、端末装置100又は200に着脱可能な記録媒体であれば特に限定されるものではない。

【0014】

図2は、図1に示した端末装置100又は200の概略構成を示すブロック図である。

【0015】

端末装置100又は200は、出力部202と、入力部204と、送受信部206と、メモリ208と、記録媒体制御部212と、制御部214と、により構成されており、各部はバス216によって接続されている。

【0016】

出力部 2 0 2 は、液晶表示装置等により構成されており、制御部 2 1 4 から出力命令されたデータを表示する。

【 0 0 1 7 】

入力部 2 0 4 は、タッチパネル、または数字入力キーなどの入力機能を備えたキーボード等により構成されており、タッチパネルで押下された位置の座標情報、またはキーボード等のキー操作信号を制御部 2 1 4 に出力する。

【 0 0 1 8 】

送受信部 2 0 6 は、アンテナ等が接続されており、制御部 2 1 4 の制御により外部から信号を受信又は外部へ信号を送信する。

【 0 0 1 9 】

メモリ 2 0 8 は、入力部 2 0 4 により入力された入力指示及び制御部 2 1 4 によりなされた処理内容を一時格納するデータ格納機能と、制御部 2 1 4 により実行される各種処理プログラムや各種アプリケーションプログラムを格納するプログラム管理機能とにより構成されている。

【 0 0 2 0 】

記録媒体制御部 2 1 2 は、端末装置 1 0 0 又は 2 0 0 に装備されているスロット（図示せず）に記録媒体 3 0 0 が差し込まれることにより、インターフェース 2 1 8 を介して記録媒体 3 0 0 の利用を制御する。

【 0 0 2 1 】

制御部 2 1 4 は、上述した出力部 2 0 2、入力部 2 0 4、送受信部 2 0 6、メモリ 2 0 8、記録媒体制御部 2 1 2 に接続されており、上述した各部の制御を行う。この制御部 2 1 4 及びその各部は、例えば ROM や RAM 等のコンピュータ読み取り可能な記録媒体（図示せず）に格納されたプログラムを CPU（Central Processing Unit）が読み取って実行することによって具現化される。

【 0 0 2 2 】

以上のような端末装置 1 0 0 又は 2 0 0 に対して着脱可能な記録媒体 3 0 0 の第一実施形態について図 3 から図 6 を参照して説明する。

【 0 0 2 3 】

図 3 は、記録媒体 3 0 0 の第一実施形態である記録媒体 3 0 0 A のブロック図

である。

【0024】

記録媒体300Aは、認証情報設定部320と処理手段設定部322からなる設定部303と、第1記憶部306と第2記憶部314からなる記憶部305と、受付部309と、認証部312と処理部315からなる制御部308と、を備えている。

【0025】

受付部309は、記録媒体300Aに入力された使用者情報を受付ける。使用者情報とは、具体的には、1以上の数字又はアルファベット等の組合せ、指紋情報、声紋情報、虹彩情報、輪郭情報及びDNA情報などの記録媒体300Aの使用者が有する情報である。この入力情報は、端末装置100又は200を利用して入力してもよいし、記録媒体300A自体に入力機能を設けて入力する構成としてもよい。

【0026】

次に、第1記憶部306と第2記憶部314に格納される情報について、図4を参照して詳細に説明する。

【0027】

第1記憶部306は、記録媒体300Aの使用の可否を決定する複数の認証情報を記憶している。また、この認証情報は、後述する第2記憶部314に格納されている処理手段に関する情報にも対応している。具体的には、この認証情報は、1以上の数字又はアルファベット等の組合せ、指紋情報、声紋情報、虹彩情報、輪郭情報及びDNA情報などにより実現可能となる。また、認証情報はこれらの複数の組合せとすることも可能である。これにより、後述する処理手段の内容に対応して、高度な認証を行うことが可能になる。

【0028】

第2記憶部314は、第1記憶部306の複数の認証情報に対応し、後述する処理手段に関する情報を格納している。処理手段とは、記録媒体300Aのメモリ（図示せず）に記憶したデータへのアクセス、ゲーム機能などである。ここで、記憶したデータに複数の領域（メモリA、メモリBなど）を設け、記憶したデー

タの内容に応じた認証情報を設定することも可能である。なお、第2記憶部314は、端末100又は200側に設けることも装置可能である。

【0029】

設定部303は、認証情報設定部320と処理手段設定部322とによって構成されている。認証情報設定部320は第1記憶部306の認証情報を設定する。処理手段設定部322は第2記憶部314の処理手段を設定する。なお、設定部303が行う設定は、外部の装置を用いて設定することも可能である。

【0030】

次に、認証部312は、上述した受付部309から得られる使用者情報310と上述した第1記憶部306に記憶された認証情報313との認証を行う。なお、認証部312は、端末装置100又は200側に設けることも可能である。

【0031】

処理部315は、上述した認証部312の認証の内容に応じて、第2記憶部の処理手段の内容を実行する。なお、処理部315は、端末装置100又は200側に設けることも可能である。

【0032】

以上のような構成において、入力された使用者情報と認証情報との認証を行い、認証が可能な場合に、認証情報に対応する予め設定された処理手段を実行する第一実施形態の動作について図5から図6を参照して説明する。

【0033】

図5は、記録媒体300Aの設定部303により第1記憶部の認証情報及び第2記憶部の処理手段を設定するフローチャートである。この処理において、まず、設定部303の認証情報設定部320は第1記憶部の認証情報を設定する(S1)。次に、設定部303の処理手段設定部322は、設定した認証情報に対応した処理手段を設定する(S2)。なお、この処理は、先に処理手段を設定し、その後処理手段に対応した認証情報を設定する手順とすることも可能である。

【0034】

図6は、記録媒体300Aの処理手順を示すフローチャートである。まず、受付部309が記録媒体300Aの使用者情報を受付ける(S11)。次に、認証部

312において、第1記憶部に記憶された認証情報と使用者情報とが一致するかどうかを認証する(S12)。認証情報と使用者情報とが一致する場合には、処理部315は、第2記憶部に設定された認証情報に対応した処理手段を実行する(S13)。ここで、図4を参照しながら、処理手段と認証情報の対応について説明する。例えば、使用者がPW3と同様の内容の使用者情報を入力した場合は、メモリAとメモリBの使用が可能になる。一方、使用者がPW2と同様の内容の使用者情報を入力した場合は、メモリAとゲームの使用が可能になる。ここで、メモリAとメモリBには重要度が異なる情報を記憶することにより、情報の重要度に対応した認証情報を設定することが可能になる。一方、認証情報と使用者情報とが一致しない場合には、使用者が入力した使用者情報が第1記憶部の認証情報と一致しない旨を出力する(S14)。さらに、第1記憶部の認証情報から、認証情報の不要な処理手段の有無を検索する(S15)。認証情報の不要な処理手段とは、図4においては、認証情報なしに対応するメモリAの使用を可能にする処理手段に該当する。ここで、認証情報の不要な処理手段がある場合には、対応する第2記憶部の処理手段を実行する(S16)。一方、認証情報の不要な処理手段がない場合には、そのまま終了する。認証情報の不要な処理手段とは、認証情報を設定する必要のない処理手段をいう。なお、ステップ14からステップ16は、必須ではなく省略することも可能である。

【0035】

次に、端末装置100又は200に対して着脱可能な記録媒体300の第二実施形態について図7から図9を参照して説明する。

【0036】

図7は、記録媒体300の第二実施形態である記録媒体300Bのブロック図である。

【0037】

第二実施形態は第一実施形態である300Aに加えて、第3記憶部402若しくは第4記憶部405と、選択部408と、通信情報設定部410とを有する。第一実施形態において説明した内容については、説明が重複するため省略する。

【0038】

第3記憶部402又は第4記憶部405に格納される情報について、図8又図9を参照して詳細に説明する。

【0039】

第3記憶部402は、図8に示すように、第1記憶部306・第2記憶部314に対応した、端末装置100又は200の通信機能を使用するための通信情報を記憶する。ここで、通信情報とは、例えば、電話番号をある関数で変換した情報などである。これによって、第三者が第3記憶部の情報を取得した場合であっても、容易に電話番号を認識することができず、第三者の不正使用の防止を図ることができる。ある関数は、端末装置に対して、通信情報を利用して通信機能を提供する業者が保持することも可能である。また、上述した電話番号をある関数で変換した情報以外にも、通信情報の保有者が予め自己の認識しうる情報に変更しておくことも可能である。この場合であっても、第三者の不正使用の防止を図ることができる。

【0040】

第4記憶部405は、図9に示すように、上述した通信情報を複数記憶する。これにより、一個人が複数の通信情報を必要とする場合であっても、複数の通信情報を一つの記録媒体に記憶することが可能になり、利便性を向上させることができる。以下、この第二実施形態では、第4記憶部を用いて説明する。

【0041】

次に、選択部408は、上述した第4記憶部405から所望の通信情報を選択する。但し、この選択部408は、端末装置100又は200若しくは外部の装置を用いて行うことも可能である。

【0042】

通信情報設定部410は、上述した第3記憶部402若しくは第4記憶部405に所望の通信情報を設定する。これにより、新しい通信情報が必要になった場合又は第4記憶部に記憶された通信情報が不要になった場合に第4記憶部の設定内容を変更することが可能になる。

【0043】

以上のような構成において、所望の通信情報を選択し、入力された認証情報と

選択された通信情報に対応する処理手段を実行する第二実施形態の動作について図10から図11を参照して説明する。

【0044】

図10は、記録媒体300Bの設定部303により、第1記憶部306の認証情報、第2記憶部314の処理手段、第3記憶部402又は第4記憶部の通信情報を設定するフローチャートである。この処理において、まず、設定部303の通信情報設定部410は、第3記憶部402又は第4記憶部405に一つ又は少なくとも一つ以上の通信情報を設定する(S21)。次に、第3記憶部402又は第4記憶部405に対応して、設定部303の認証情報設定部320は、第1記憶部306の認証情報を設定する(S22)。次に、設定部303の処理手段設定部322は、設定した通信情報と認証情報に対応した処理手段を設定する(S23)。なお、第1記憶部306の認証情報と第2記憶部314の処理手段と、第3記憶部402又は第4記憶部405の通信情報の設定は、どのような順番で設定することも可能である。

【0045】

ここで、第2記憶部に記憶される処理手段の内容について詳細に説明する。処理手段は、通信機能、電子商取引機能、電子財布機能、メモリ機能、ナビゲーションシステム機能等により構成される。

【0046】

また、通信機能においては、通話機能、電子メール機能又は着信機能のみなどを選択することも可能であり、機能の内容に対応した認証情報を設定することも可能である。また、通信機能を使用する際には、通話機能の課金に上限を設け、その上限に対応した認証情報を設定することも可能である。

【0047】

また、電子商取引機能においても、電子商取引の対象や金額の設定に応じて認証情報を設定することも可能である。

【0048】

また、電子財布機能においては、預金、残高照会、引き落としなどの機能に応じた認証情報を設定することも可能である。

【 0 0 4 9 】

また、メモリ機能においては、通信機能を利用して取得した情報を、情報の重要度に応じて認証情報を設定することも可能である。

【 0 0 5 0 】

図 1 1 は、記録媒体 3 0 0 B の処理手順を示すフローチャートである。

【 0 0 5 1 】

まず、選択部 4 0 8 は、第 4 記憶部 4 0 5 に記憶された通信情報から所望の通信情報を選択する (S3 1)。次に、受付部 3 0 9 が記録媒体 3 0 0 B の使用者情報を受付ける (S3 2)。次に、認証部 3 1 2 において、第 1 記憶部 3 0 6 に記憶された認証情報と使用者情報とが一致するか否かを認証する (S3 3)。認証情報と使用者情報とが一致する場合には、選択部 4 0 8 により選択された通信情報と認証部 3 1 2 により認証された認証情報に対応した第 2 記憶部 3 1 4 に記憶された処理手段の実行を可能にする (S3 4)。ここで、図 9 を参照しながら、処理手段の実行内容について説明する。例えば、使用者が法人の通信情報を選択し、さらに PW1 と同様の内容の使用者情報を入力した場合は、端末装置 1 0 0 又は 2 0 0 の通信機能を実行可能にする処理を行う。さらに、使用者が上記通信機能に加えて、電子商取引の機能を実行可能にするためには、使用者が PW1 の代わりに PW2 を使用者情報として入力するという簡単な手段で電子商取引の機能を実行可能にすることができる。なお、図 9 においては、それぞれ異なる認証情報を設定したが、使用者の要望に応じて、同じ認証情報を設定することも可能である。一方、認証情報と使用者情報とが一致しない場合には、認証情報と使用者情報が一致しない旨を出力する (S3 5)。さらに、第 1 記憶部の認証情報から、認証情報の不要な処理手段の有無を検索する (S3 6)。ここで、認証情報の不要な処理手段がある場合には、対応する第 2 記憶部の処理手段を実行する (S3 7)。認証情報の不要な処理手段とは、図 9 においては、法人の通信情報を選択した場合には、認証情報なしに対応するメモリ B の使用を可能にする処理手段に該当する。一方、認証情報の不要な処理手段がない場合には、そのまま終了する。なお、ステップ 5 からステップ 8 は必須ではなく、省略することも可能である。

【 0 0 5 2 】

次に、端末装置 1 0 0 又は 2 0 0 に対して着脱可能な記録媒体 3 0 0 の第三実施形態について図 1 2 から図 1 3 を参照して説明する。

【 0 0 5 3 】

図 1 2 は、記録媒体 3 0 0 の第三実施形態である記録媒体 3 0 0 C のブロック図である。

【 0 0 5 4 】

第三実施形態は第一実施形態である 3 0 0 A 又は第二実施形態である 3 0 0 B に加えて、判断部 6 0 2 を有する。第一実施形態又は第二実施形態において説明した内容については、説明が重複するため省略する。

【 0 0 5 5 】

判断部 6 0 2 は、着脱検出信号 INS 6 0 4 を利用して、端末装置 1 0 0 又は 2 0 0 と記録媒体 3 0 0 C の着脱を検出する。

【 0 0 5 6 】

着脱検出信号 INS 6 0 4 の信号線の一端は記録媒体内部ではグランド V s s 6 0 6 に接続されている。そして着脱検出信号 INS 6 0 4 の信号線他端は、この記録媒体 3 0 0 C に装着される端末装置 1 0 0 又は 2 0 0 において、プルアップ抵抗 R 6 0 5 を介し端末装置内の電源に接続されている。さらに、グランド V s s 6 0 6 の信号線は、この記録媒体が挿入される端末装置 1 0 0 又は 2 0 0 内のグランドに接続されるように構成されている。この構成により、端末装置 1 0 0 又は 2 0 0 の電源電圧 V d d 6 0 3 を利用して記録媒体 3 0 0 C が装着される端末装置 1 0 0 又は 2 0 0 からの着脱状態を検出することが可能になる。

【 0 0 5 7 】

以上のような構成において、端末装置が記録媒体から抜き出されたことを認識した後、記録媒体を使用する場合に、認証を行うことにより記録媒体の不正使用を防止する第三実施形態の動作について図 1 3 から図 1 4 を参照して説明する。

【 0 0 5 8 】

図 1 3 は、端末装置 1 0 0 又は 2 0 0 から記録媒体 3 0 0 C の着脱を検出する処理を示すフローチャートである。この処理において、まず、検出部 5 2 2 は、着脱検出信号 INS 5 0 4 を受信することにより端末装置 1 0 0 又は 2 0 0 から記

録媒体 3 0 0 C を着脱したことを検出する (S4 1)。次に、コントローラ 5 2 6 は、検出部 5 2 2 が着脱検出信号 INS 5 0 4 を受信したことを履歴情報記録部 5 2 8 に送信する (S4 2)。次に、履歴情報記録部 5 2 8 は、履歴情報 5 2 4 として着脱検出信号 INS 5 0 4 を記録する (S4 3)。この履歴情報 5 2 4 としては、端末装置 1 0 0 又は 2 0 0 から記録媒体 3 0 0 が抜き出されたという情報に加えて、記録媒体 3 0 0 C が着脱された時間、記録媒体 3 0 0 C が着脱された場所等の情報であってもよい。

【0 0 5 9】

図 1 4 は、記録媒体 3 0 0 C の処理手順を示すフローチャートである。まず、記録媒体 3 0 0 C の履歴情報記録部 6 2 8 に履歴情報 6 2 4 が記録されているか否かを検出する (S5 1)。履歴情報が記録されている場合には、記録媒体 3 0 0 C は、パスワード等の入力を要求する (S5 2)。次に、選択部 4 0 8 は、第 4 記憶部に記憶された通信情報から所望の通信情報を選択する (S5 3)。次に、受付部 3 0 9 が記録媒体 3 0 0 C の使用者情報を受信する (S5 4)。次に、認証部 3 1 2 において、第 1 記憶部に記憶された認証情報と使用者情報とが一致するか否かを認証する (S5 5)。認証情報と使用者情報とが一致する場合には、選択部 4 0 8 により選択された通信情報と認証部 3 1 2 により認証がなされた認証情報に対応した第 2 記憶部に記憶された処理手段の実行を可能にする (S5 6)。

【0 0 6 0】

一方、認証情報と使用者情報とが一致しない場合には、認証情報と使用者情報が一致しない旨を出力する (S5 7)。さらに、第 1 記憶部と第 2 記憶部から、認証情報の不要な処理手段の有無を検索する (S5 8)。ここで、認証情報の不要な処理手段がある場合には、その処理手段を実行する (S5 9)。一方、認証情報の不要な処理手段がない場合には、そのまま終了する。なお、ステップ 5 7 からステップ 5 9 は必須ではなく、省略することも可能である。

【0 0 6 1】

【発明の効果】

以上説明したように、この発明によれば、処理手段の内容に対応した認証情報

を設定することが可能になるため、効率良く処理手段の内容に対応して効率良く第三者の使用を防止することが可能になる。

【 0 0 6 2 】

また、一つの記録媒体に複数の通信情報を複数記憶するため、一個人が複数の通信情報を有する場合であっても、複数の記録媒体を携帯する必要がなく、紛失又は盗難による不正使用の可能性を低くすることができる。

【 0 0 6 3 】

また、端末装置が記録媒体が着脱された後、記録媒体が使用される場合には、必ず認証が行われるため、第三者により記録媒体が端末装置から抜き出された場合であっても再度認証を行うため、不正使用を防止することが可能になる。

【図面の簡単な説明】

【図 1】

この発明の一実施の形態に係る端末装置から着脱可能な記録媒体の不正使用防止システムの概略構成を示す図

【図 2】

端末装置の概略構成を示す図

【図 3】

第一実施形態に係る記録媒体の概略構成を示すブロック図

【図 4】

第一実施形態に係る第 1、2 記憶部の内容を説明する図

【図 5】

第一実施形態に係る設定部の処理手順を設定するフローチャート

【図 6】

第一実施形態に係る記録媒体の処理手順を説明するフローチャート

【図 7】

第二実施形態に係る記録媒体の概略構成を示すブロック図

【図 8】

第二実施形態に係る第 1、2、3 記憶部の内容を説明する図

【図 9】

第二実施形態に係る第 1、2、4 記憶部の内容を説明する図

【図 1 0】

第二実施形態に係る設定部の処理手順を設定するフローチャート

【図 1 1】

第二実施形態に係る記録媒体の処理手順を説明するフローチャート

【図 1 2】

第三実施形態に係る記録媒体の概略構成を示すブロック図

【図 1 3】

端末装置と記録媒体との着脱を検出する処理を示すフローチャート

【図 1 4】

第三実施形態に係る記録媒体の処理手順を説明するフローチャート

【符号の説明】

1 0 0, 2 0 0 端末装置

3 0 6 第 1 記憶部

3 1 2 認証部

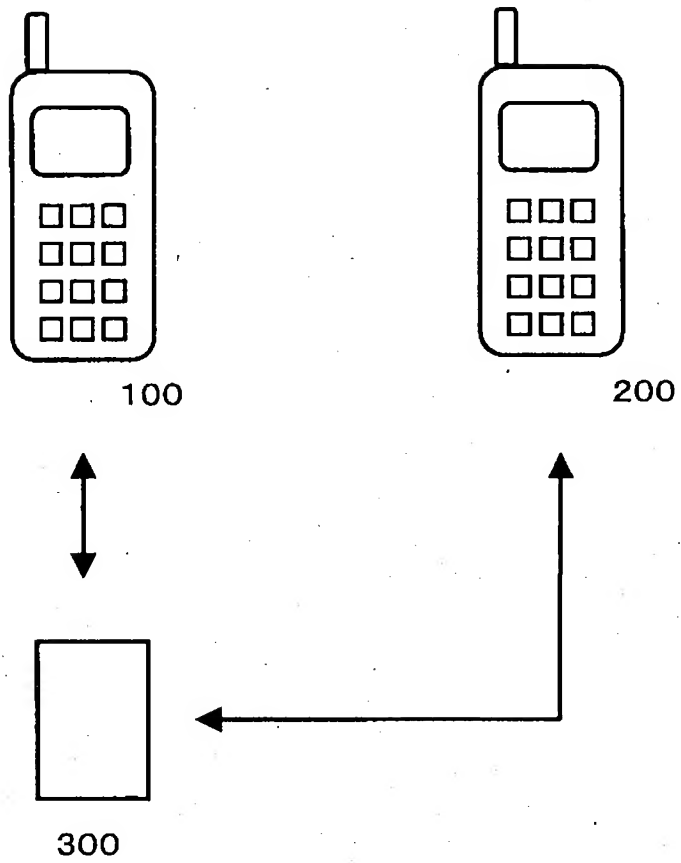
3 1 4 第 2 記憶部

3 1 5 処理部

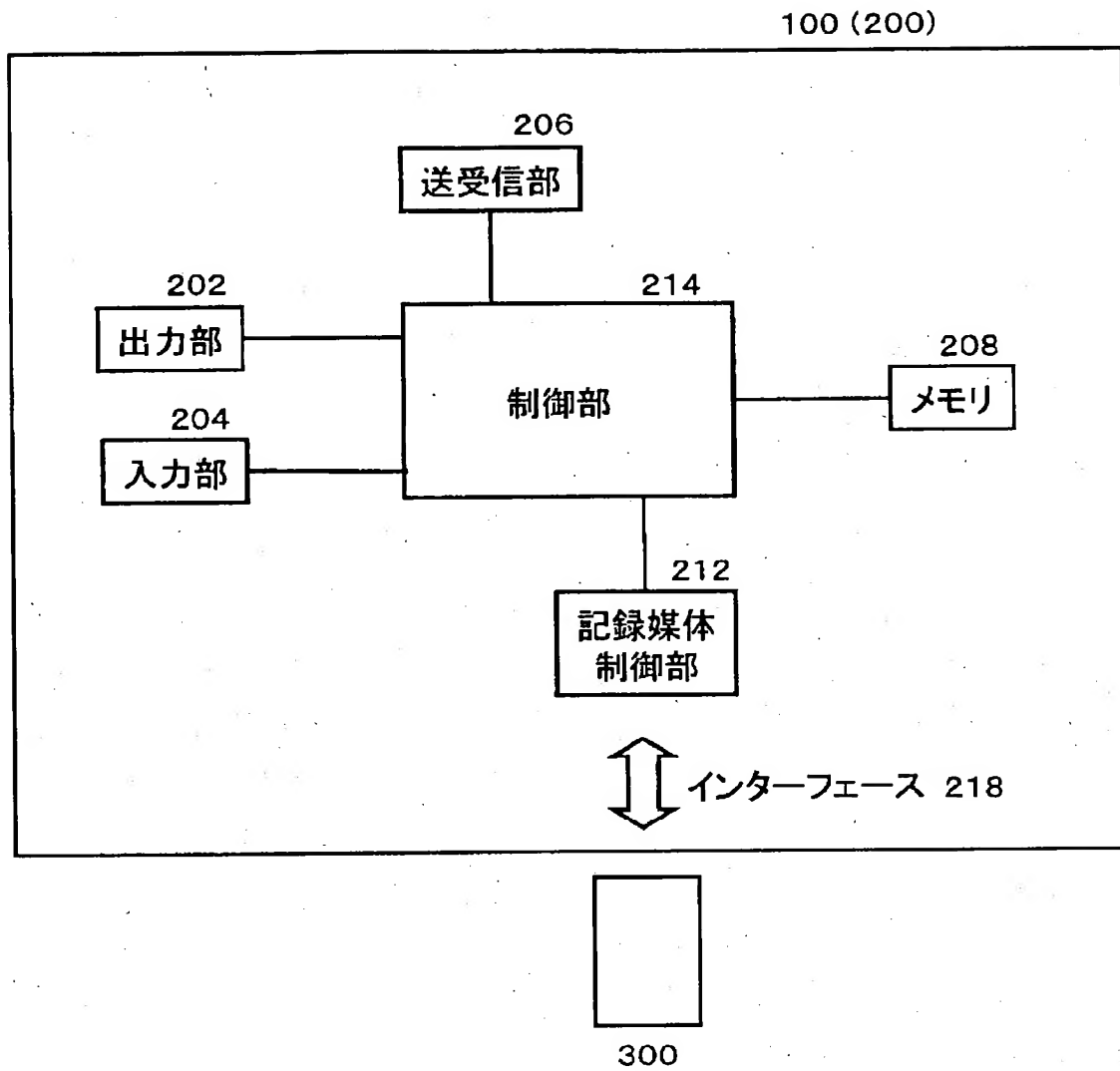
【書類名】

図面

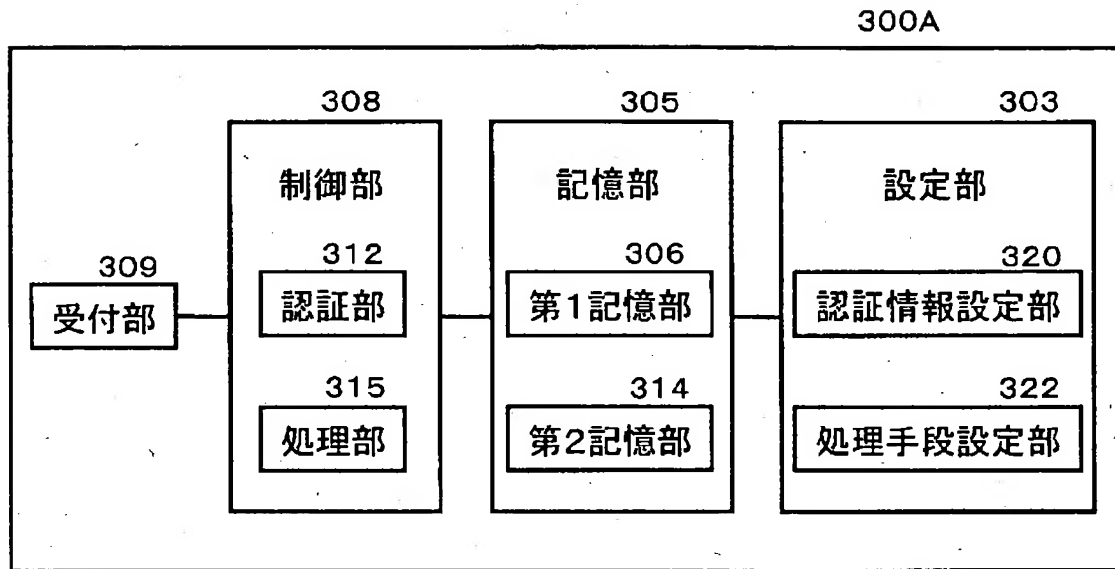
【図 1】



【図 2】



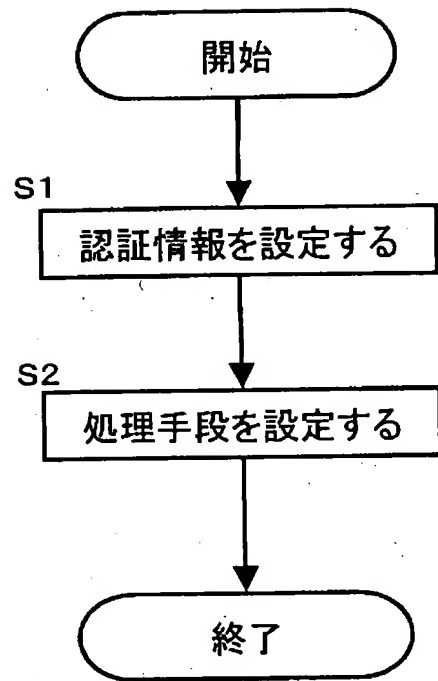
【図3】



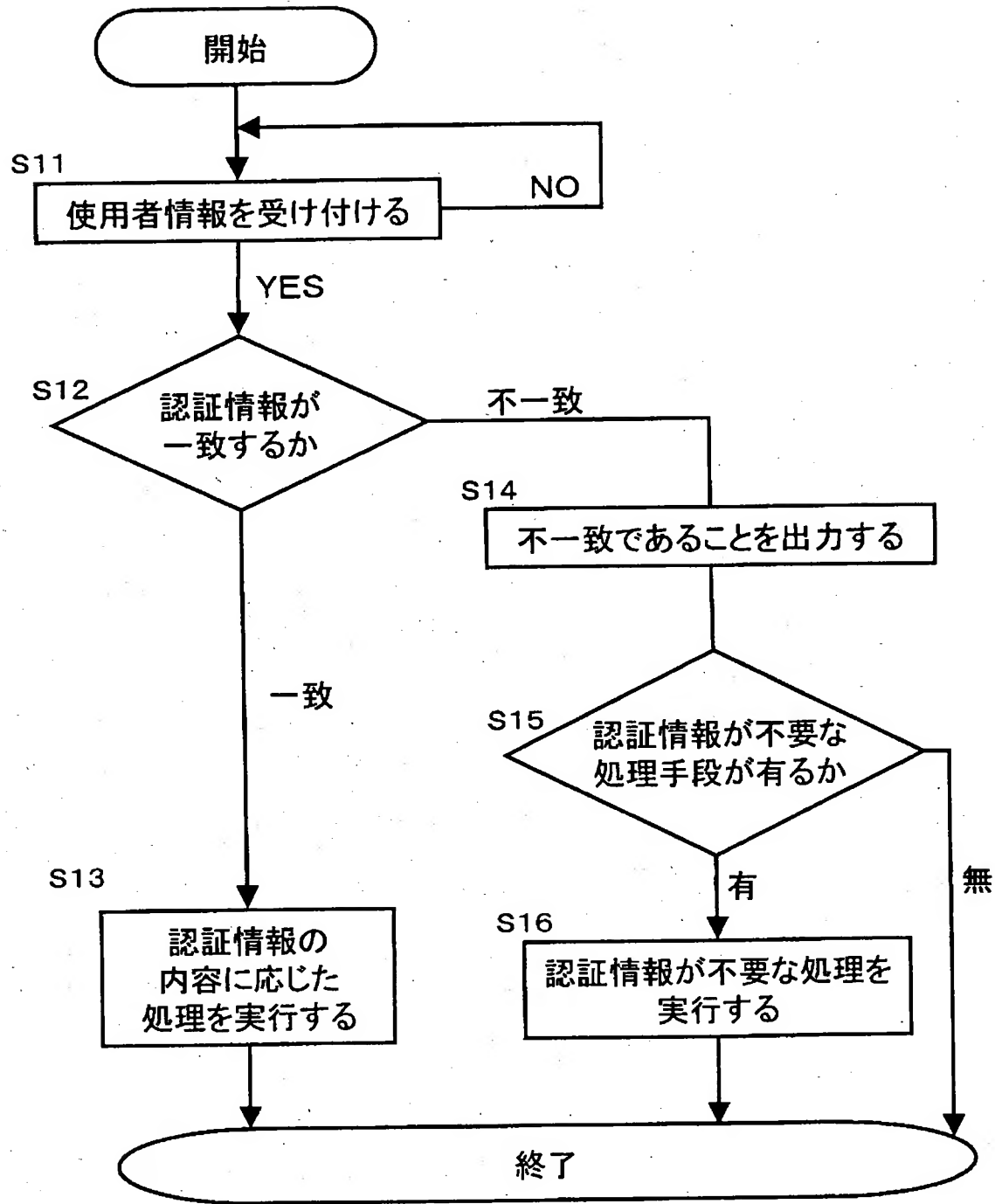
【図4】

第1記憶部	第2記憶部
認証情報	処理手段
なし	メモリ A
PW1	メモリ A+B
PW2	メモリ A, ゲーム
PW3	メモリ A+B, ゲーム

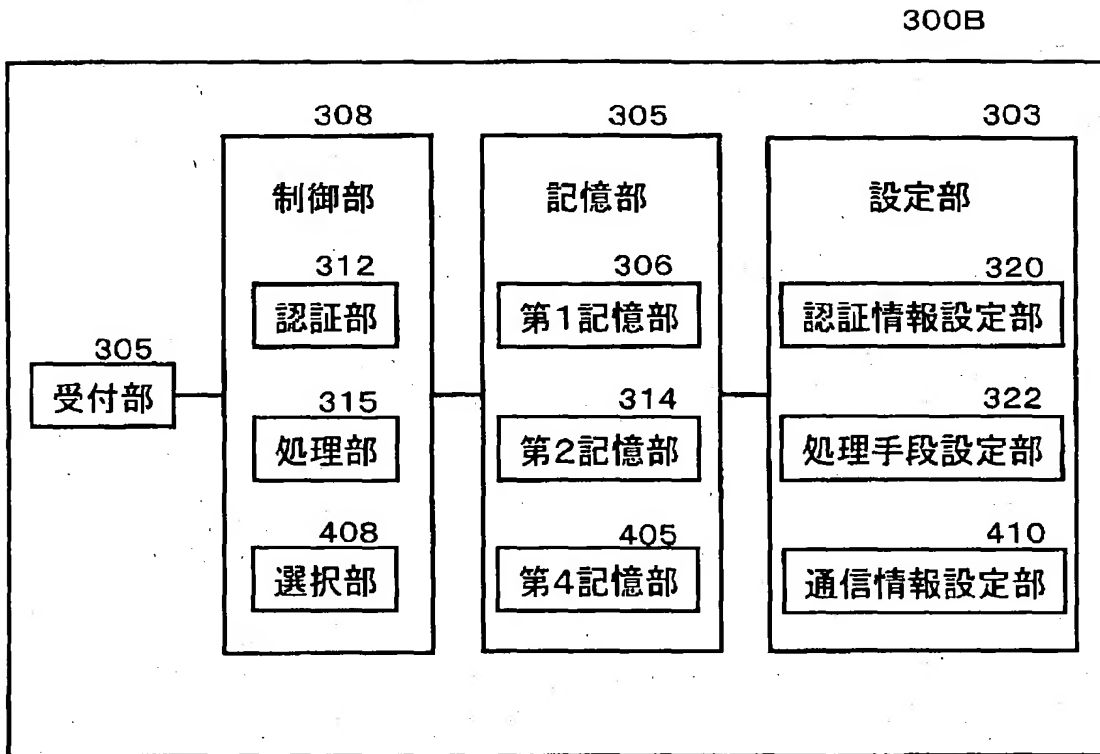
【図 5】



【図6】



【図 7】



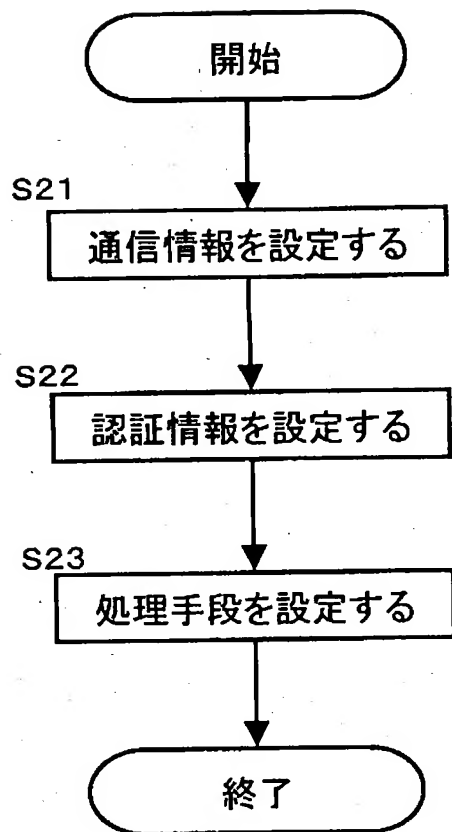
【図 8】

第3記憶部	第1記憶部	第2記憶部
通信情報	認証情報	処理手段
〇〇〇	なし	メモリ A
-〇〇〇〇	PW1	メモリ A+B
-〇〇〇〇	PW2	メモリ A+B, 通信機能
	PW3	メモリ A+B, 通信機能, 電子商取引

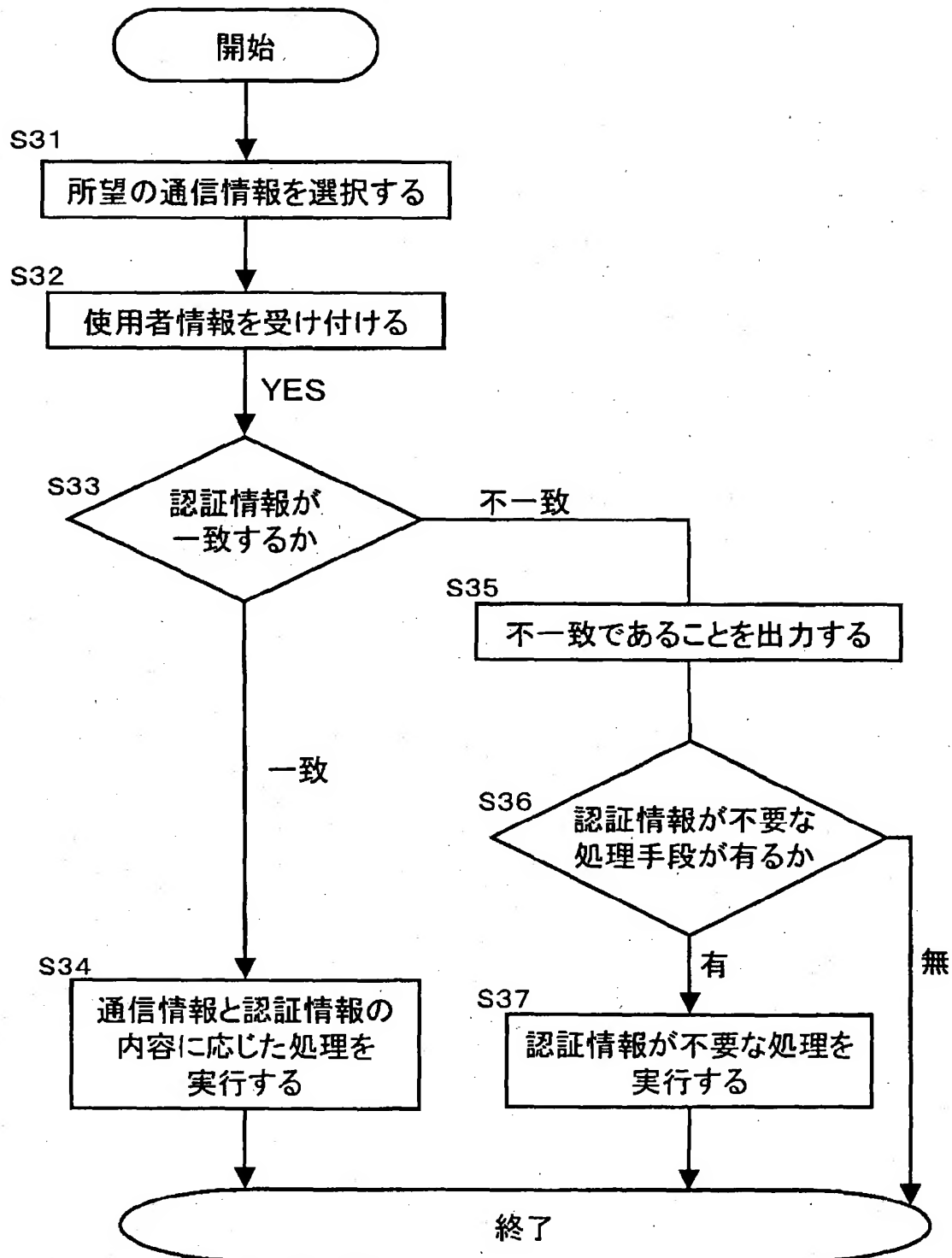
【図9】

第4記憶部	第1記憶部	第2記憶部
通信情報	認証情報	処理手段
○○○-○○○-○○○○ (法人)	PW1	通信機能
	PW2	通信機能 + 電子商取引
	なし	メモリ B
△△△-△△△-△△△△ (個人1)	PW3	メモリ A + メモリ B
	PW4	メモリ A, B + 通信機能
×××-×××-×××× (個人2)	PW5	通信機能
	なし	メモリ A

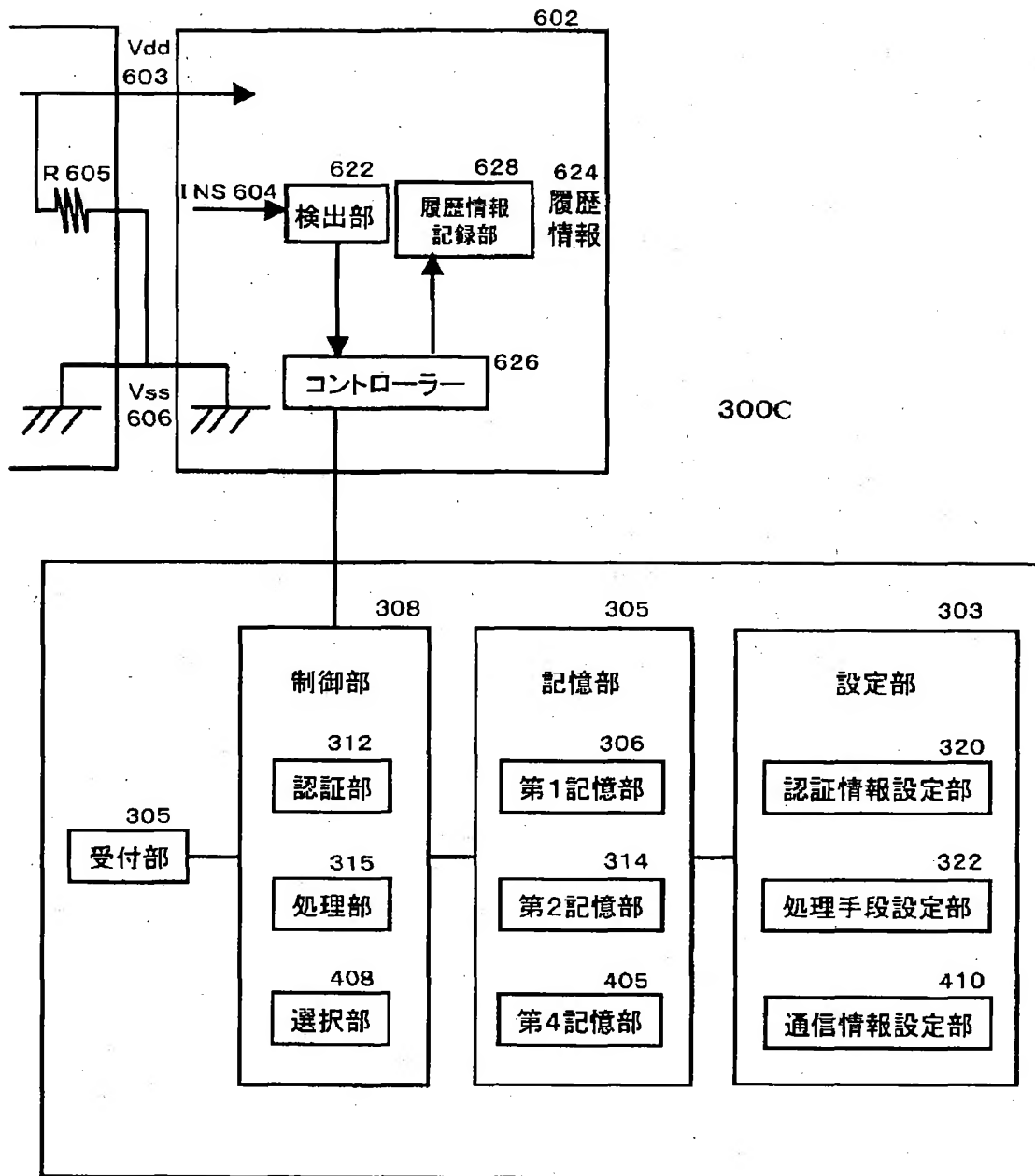
【図10】



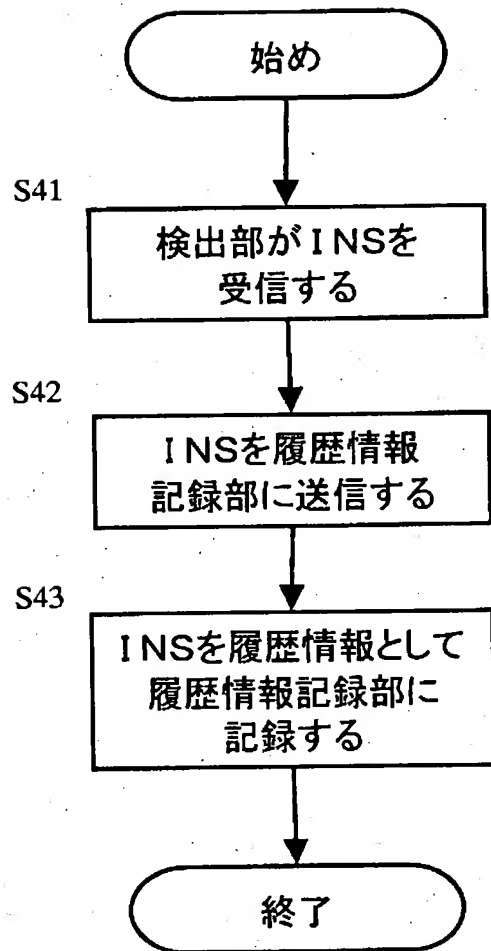
【図11】



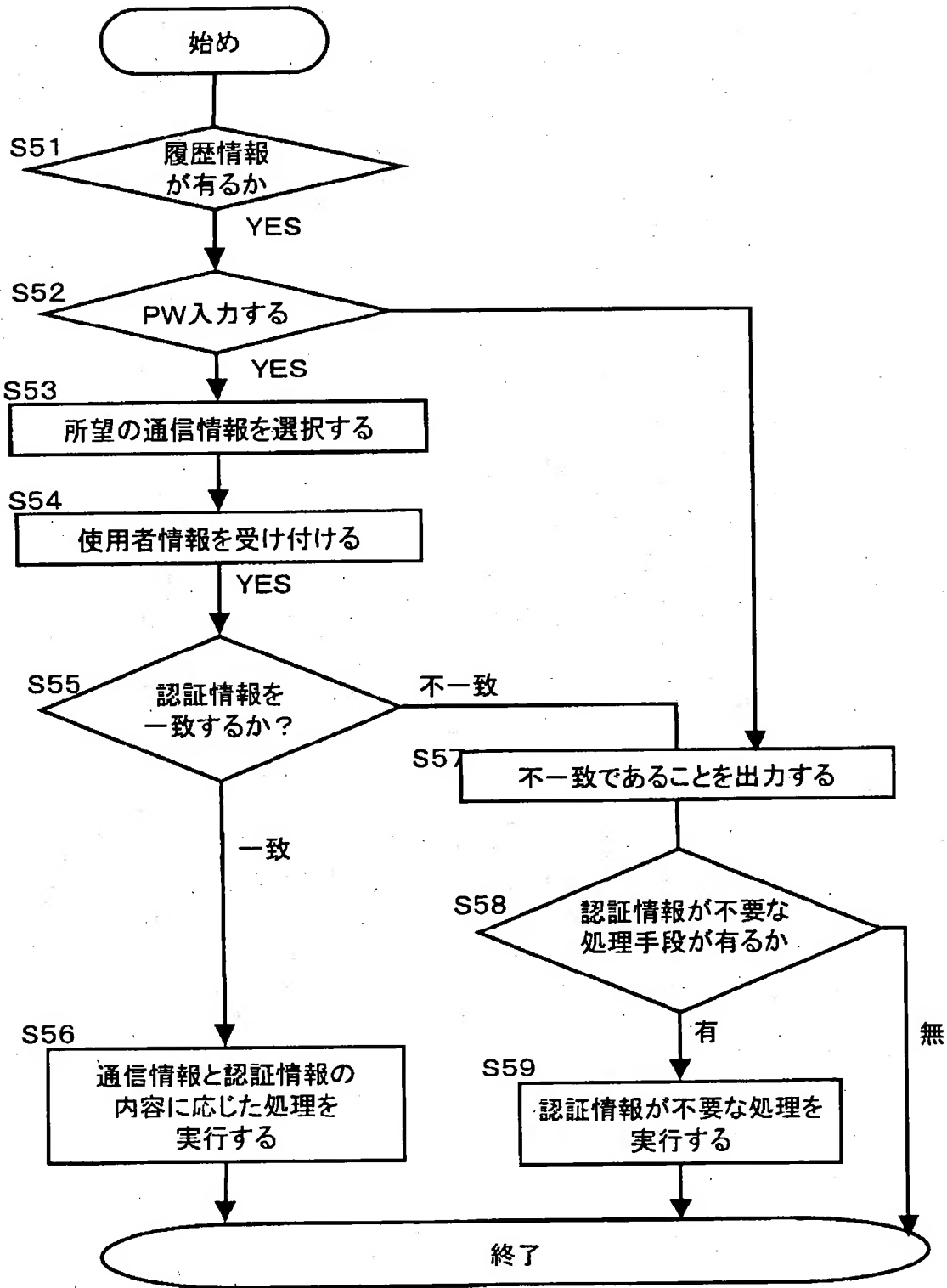
【図12】



【図13】



【図14】



【書類名】 要約書

【要約】

【課題】 端末装置に着脱可能な記録媒体の不正使用を防止し、かつ利便性の高い記録媒体不正使用防止システムを提供する。

【解決手段】 端末装置に着脱可能な記録媒体の不正使用防止システムは、記録媒体の使用の可否を決定する認証情報を複数記憶する第1記憶部と、第1記憶部に記憶された認証情報に対応した処理手段を記憶する第2記憶部と、端末装置の通信機能を使用するための通信情報を複数記憶する第4記憶部と、第4記憶部の通信情報から所望の通信情報を選択する選択部と、記録媒体の利用者が有する利用者情報と認証情報との認証を行う認証部と、選択部により選択された通信情報と認証部の認証の内容とに対応した処理手段を実行する処理部と、を備える。

【選択図】 図9

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社